UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

In re: *Data Security Cases Against NELNET SERVICING, LLC*	**Case No. 4:22-cv-3191** **The Honorable John M. Gerrard, U.S.D.J.** **The Honorable Cheryl R. Zwart, U.S.M.J.** **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Ian Scott, Jessica Alexander, Pamela Bump, Bridget Cahill, Lesly Canales, Melissa Charbonneau, Douglas Conley, Noah Helvey, Dallin Iler, Dustin Jones, Kayli Lazarz, Brittni Linn, Delilah Oliveira, Devinne Peterson, Eric Polanco, Justin Randall, Sofia Rodriguez, Joshua Sanchez, Charles Sangmeister, William Spearman, Taylor Vetter, Rachel Woods, Garner J. Kohrell, Olivia Covington, Alexis Luna, and Mary Traynor ("Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendants Nelnet Servicing, LLC ("Nelnet") and EdFinancial Services, LLC ("EdFinancial") (collectively with EdFinancial and Nelnet, "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, names, addresses, email addresses, phone numbers, and Social Security numbers (collectively "PII"); (ii) failure to comply with industry standards to protect information systems that contain PII; (iii) unlawful disclosure of Plaintiffs' and Class Members' PII; and (iv)

failure to provide adequate notice to Plaintiffs and other Class Members that their PII had been disclosed and compromised.

2. Nelnet is one of the largest student loan servicers in the United States, servicing $589 billion in student loans for over 17 million borrowers.

3. In addition to servicing student loans, Nelnet provides online technology services such as web portal and payment processing services to other student loan servicers, including EdFinancial and the Oklahoma Student Loan Authority ("OSLA").

4. On or around August 26, 2022, Nelnet began publicly notifying state Attorneys General and approximately 2,501,324 impacted student borrowers of OSLA and EdFinancial that their PII had been accessed and stolen by an unauthorized third-party (the "Data Breach").

5. By August 26, 2022, Nelnet had known of the Data Breach for well over a month but had failed to notify a single impacted individual. Nelnet chose to notify individuals via U.S Mail in letters entitled "Notice of Security Incident."

6. As a result of Nelnet's failures and lax security protocols, EdFinancial's entrustment of Nelnet with their borrowers' sensitive PII, hackers gained access to Nelnet's computer systems and/or servers and were able to steal the personal information of millions of customers, including their Social Security numbers, phone numbers, emails, and addresses.

7. The Data Breach was a direct and proximate result of Nelnet's flawed online system configuration and design and Nelnet's failure to implement and follow basic security procedures.

8. Because of Nelnet's failures, unauthorized individuals were able to access and pilfer Plaintiffs' and Class Members' PII.

9. As a result, Plaintiffs and Class Members are at substantially increased risk of future identity theft, both currently and for the indefinite future. Plaintiffs' and Class Members'

PII, including their Social Security numbers, that were compromised by cyber criminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft.

10. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, breach of confidence, invasion of privacy—intrusion upon seclusion, violations of consumer protection statutes of their home states, violations of data protection statutes of their home states, and injunctive relief claims.

11. Plaintiffs seek damages and injunctive relief requiring Nelnet to adopt reasonably sufficient practices to safeguard the PII that remains in Nelnet's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

12. Given that information relating to the Data Breach, including the systems that were impacted, the configuration and design of Defendant's website and systems remain exclusively in Defendant's control, Plaintiffs anticipate additional support for their claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class and Subclass exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Members of the Class and Subclass defined below, and a significant portion of putative Class and Subclass Members are citizens of a different state than Defendant.

14. This Court has personal jurisdiction over Defendant Nelnet because Defendant Nelnet is a resident of the State of Nebraska.

15. This Court has personal jurisdiction over Defendants EdFinancial because EdFinancial conducts substantial business in Nebraska and this District through their contractual relationship with Defendant Nelnet and have continuous and systematic contact with the state of Nebraska.

16. This Court also has specific personal jurisdiction over Defendants related to this action because Plaintiffs' claim arises out of Defendants' contacts with and student loan servicing business in this state and district.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District

18. Plaintiffs' claims also arise out of or relate to Defendants' contacts with California. Defendants have intentionally created extensive contacts with California through its deliberate marketing and sale of its services in the forum.

PARTIES

I. Plaintiffs

19. Plaintiff Ian Scott ("Plaintiff Scott") is a citizen and resident of the State of New Mexico.

20. Plaintiff Jessica Alexander ("Plaintiff Alexander") is a citizen and resident of the State of California.

21. Plaintiff Pamela Bump ("Plaintiff Bump") is a citizen and resident of the Commonwealth of Massachusetts.

22. Plaintiff Bridget Cahill ("Plaintiff Cahill") is a citizen and resident of the Commonwealth of Massachusetts.

23. Plaintiff Lesly Canales ("Plaintiff Canales") is a citizen and resident of the State of New York.

24. Plaintiff Melissa Charbonneau ("Plaintiff Charbonneau") is a citizen and resident of the State of Illinois.

25. Plaintiff Douglas Conley ("Plaintiff Conley") is a citizen and resident of the State of Arizona.

26. Plaintiff Noah Helvey ("Plaintiff Helvey") is a citizen and resident of the State of Utah.

27. Plaintiff Dallin Iler ("Plaintiff Iler") is a citizen and resident of the State of Indiana.

28. Plaintiff Dustin Jones ("Plaintiff Jones") is a citizen and resident of the Commonwealth of Pennsylvania.

29. Plaintiff Kayli Lazarz ("Plaintiff Lazarz") is a citizen and resident of the State of Colorado.

30. Plaintiff Brittni Linn ("Plaintiff Linn") is a citizen and resident of the Commonwealth of Pennsylvania

31. Plaintiff Delilah Oliveira ("Plaintiff Oliveira") is a citizen and resident of the Commonwealth of Massachusetts.

32. Plaintiff Devinne Peterson ("Plaintiff Peterson") is a citizen and resident of the Commonwealth of Pennsylvania.

33. Plaintiff Eric Polanco ("Plaintiff Polanco") is a citizen and resident of the State of California and was previously a resident of the Commonwealth of Massachusetts.

34. Plaintiff Justin Randall ("Plaintiff Randall") is a citizen and resident of the State of Wisconsin.

35. Plaintiff Sofia Rodriguez ("Plaintiff Rodriguez") is a citizen and resident of the State of Michigan.

36. Plaintiff Joshua Sanchez ("Plaintiff Sanchez") is a citizen and resident of the State of Florida.

37. Plaintiff Charles Sangmeister ("Plaintiff Sangmeister") is a citizen and resident of the State of California.

38. Plaintiff William Spearman ("Plaintiff Spearman") is a citizen and resident of the State of South Carolina.

39. Plaintiff Taylor Vetter ("Plaintiff Vetter") is a citizen and resident of the State of New York.

40. Plaintiff Rachel Woods ("Plaintiff Woods") is a citizen and resident of the State of Texas.

41. Plaintiff Garner J. Kohrell ("Plaintiff Kohrell") is a citizen and resident of the State of Minnesota.

42. Plaintiff Olivia Covington ("Plaintiff Covington") is a citizen and resident of the Commonwealth of Virginia.

43. Plaintiff Alexis Luna ("Plaintiff Luna") is a citizen and resident of the State of California.

44. Plaintiff Mary Traynor ("Plaintiff Traynor") is a citizen and resident of the State of Illinois.

II. Defendants

45. Defendant Nelnet Servicing, LLC ("Nelnet") is Nebraska limited liability company with its principal place of business located at 121 South 13th Street, Suite 100, Lincoln, Nebraska, 68508.

46. Nelnet is a Nebraska-based company which primarily "engage[s] in student loan servicing, tuition payment processing and school information systems, and communications" and primarily makes money via "net interest income earned on a portfolio of federally insured student loans."[1] As of June 30, 2022, the Nelnet was servicing $589.5 billion in loans for 17.4 million borrowers.[2]

47. Nelnet earns significant revenue providing technology services such as website portal and payment processing to other student loan servicers,[3] such EdFinancial.

48. No individual voluntarily engages Nelnet as their servicing system and customer website portal provider. Instead, Nelnet is chosen by a federal student loan servicer such as EdFinancial to provide web portal and payment processing services without any input from the individual student loan borrower.

49. Defendant EdFinancial Services, LLC ("EdFinancial") is a Nevada limited liability company with its principal place of business located at 298 N Seven Oaks Drive, Knoxville, Tennessee 37922.

50. EdFinancial is a student loan servicing company that uses Nelnet, a different student loan servicing company, as its servicing system and customer website portal provider.

---

[1] *About Us*, NELNET, https://www.nelnetinvestors.com/Home/default.aspx (accessed Sept. 6, 2022).
[2] *Nelnet 10Q Earnings Release*, NELNET (Aug. 8, 2022) https://s21.q4cdn.com/368920761/files/doc_financials/2022/q2/8K-Exhibit-99.1-8.8.22-10Q-Earnings-Release-FINAL.pdf (accessed Sept. 6, 2022).
[3] *Id.*

FACTUAL BACKGROUND

I. Nelnet Obtains, Collects, and Stores Account Holders' PII

51. Companies and organizations, including EdFinancial, hire Nelnet to provide web payment portal and processing services. Nelnet provides these services by integrating their application programming interface, or "API", into a company's or organization website/

52. Once Nelnet's API has been integrated into a company's or organization's website, Nelnet is in charge of obtaining, collecting, and storing the PII of individuals that create payment accounts via the Nelnet API.

53. Thus, individuals whose student loans are assigned to a loan servicer that has engaged Nelnet to provide web payment portal and processing services interacts with Nelnet when they create a web account and make payments, provides PII to Nelnet in connection with this process.

54. However, Plaintiffs and members of the class were completely unaware that, when they created a web payment account with their loan servicers, that they were actually dealing with and providing information to Nelnet and they first learned of this when they received the letters notifying them that Nelnet had allowed their PII to be exposed..

55. Nelnet maintains, keeps, and exploits Plaintiffs' and Class Members' PII for Nelnet's own benefit, including long after individuals have paid off their loans in full.

56. Nelnet is in complete operation, control, and supervision of its website and systems, and Nelnet intentionally configured and designed its website and systems without adequate data security protections.

57. EdFinancial entrusted Nelnet with their student loan borrowers' PII. EdFinancial did not properly verify, oversee, and supervise Nelnet's entrustment of their student loan borrowers' PII.

58. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

59. Plaintiffs and Class Members reasonably expect that student loan servicers and their vendors, such as Defendants, will use the utmost care to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

60. Nelnet acknowledges that it has an obligation to protect PII from disclosure and thus makes the following representation on the Nelnet website:

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[4]

61. Reciprocally, EdFinancial's privacy policy (the "EdFinancial Privacy Policy") says "We are committed to excellence in customer service, and your privacy is important to us."[5]

62. The EdFinancial Privacy Policy further states:

> The security of your personal information is important to us. When you enter sensitive information (such as a social security number) on our registration or order forms, we encrypt that information. We follow industry-accepted best practices for protecting personal information, both during transmission and at rest on our systems.

[4] *Nelnet Privacy Policy Mission Statement, Our Security Procedures*, NELNET, https://www.nelnet.com/privacy-and-security#:~:text=As%20stated%20above%20we%20do,Comply%20with%20the%20law (accessed March 3, 2023).
[5] *See* https://www.edfinancial.com/Privacy (last accessed March 3, 2023).

> While no method of communication over the Internet or electronic storage is ever 100% secure, we have gone to great lengths to protect your personal information through the use of firewalls, intrusion protection systems, file level encryption of data while at rest and encryption of data while in transit over our network. All systems provide extensive logging and automated reporting of issues enabling timely response, interdiction and corrective actions if necessary.[6]

63. Defendants violated their own privacy policies by unlawfully disclosing Plaintiff's and Class Members' Private Information to third parties.

64. Despite the above representations, Defendants failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

65. Had Defendants followed industry guidelines and adopted reasonably security measures as represented in their privacy policies, Defendants would have prevented intrusion into Nelnet's information systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

II. FTC Guidelines

66. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

67. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

[6] *Id.*

68. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

69. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Social Security information stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

72. Defendants was always fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Defendants were also aware of the significant repercussions that would result from its failure to do so.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

73. Beginning in June 2022, Nelnet allowed an unauthorized third-party to access Plaintiffs' and Class Members' student loan account registration information, including their names, addresses, email addresses, phone numbers, and Social Security numbers. According to Nelnet, this unauthorized access continued through July 22, 2022.

74. Nelnet did not discover the unauthorized access until July 21, 2022, when Nelnet claims to have notified EdFinancial and OSLA about the vulnerability and unauthorized access.

75. According to Nelnet, approximately 2.5 million student loan borrowers had their PII exposed as a result of the data breach. Approximately 2.25 million of the borrowers were borrowers whose loans are serviced by EdFinancial, with the remaining borrowers' loans serviced by OSLA.

76. Despite discovering the Data Breach July 21, 2022, Nelnet did not notify the U.S. Department of Education of the Data Breach until after August 17, 2022, and did not begin notifying impacted customers until August 26, 2022.

77. While the notice letters to Plaintiffs and Class Members contained the respective letterhead of EdFinancial and OSLA, the notice letters were actually sent by Nelnet.

II. Defendants' Data Security Failures Caused the Data Breach

78. Up to, and including, the period when the Data Breach occurred, Nelnet breached its duties, obligations, and promises to Plaintiffs and Class Members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers were susceptible to a data breach;

d. implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its systems that accessed customers' personal information and otherwise would have protected customers' sensitive personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented customers' sensitive personal information from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

f. adequately safeguard customers' sensitive personal information and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

79. Up to, and including, the period when the Data Breach occurred, EdFinancial breached its duties, obligations, and promises to Plaintiffs and Class Members, by its failure to verify, oversee, and supervise Nelnet's entrustment of their student loan borrowers' PII.

III. Nelnet's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

80. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

81. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

82. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

83. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

84. Prior to the Data Breach, and during the breach itself, Nelnet failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security.

Furthermore, by failing to have reasonable data security measures in place, Nelnet engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

IV. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

85. Defendants understood the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

86. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

87. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

88. The forms of PII involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with

those entities.

89. Indeed, even the Social Security Administration (''SSA") warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

90. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

91. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as

opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

92. Thus, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

93. As highly sophisticated parties that handle sensitive PII, Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

94. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

95. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

96. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit

> identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

97. Personal is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

98. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

99. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

V. The Data Breach Damaged Plaintiffs and Class Members.

100. As a result of Defendants' deficient security measures, Plaintiffs and Class Members have been harmed by the compromise of their sensitive personal information, which is likely currently for sale on the dark web and through private sale to other cyber criminals and/or being used by criminals for identify theft and other fraud-related crimes.

101. Plaintiffs and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, emails, phone numbers, and physical addresses as a result of the breach. These specific types of information are associated with a high risk of fraud.

102. Criminals have fraudulently applied for credit cards using the PII of Plaintiffs and Class Members.

103. Criminal have fraudulently filed tax returns using the PII of Plaintiffs and Class members.

104. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

105. Plaintiffs and Class Members also suffered a "loss of value" of their sensitive personal information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web—an underground market for illicit activity, including the purchase of hacked personal information—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiffs and Class Members.

106. Plaintiffs' and Class Members' stolen personal information is a valuable commodity to identity thieves. William P. Barr, former United States Attorney General, made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. One commentator confirmed, explaining that, "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud." In fact, Plaintiffs' and Class Members' personal information is currently available for purchase on the dark web and/or through private sale to other cyber criminals.

107. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain

more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

108. Plaintiffs and Class Members also suffered "benefit of the bargain" damages. Plaintiffs and Class Members overpaid for services that should have been—but were not—accompanied by adequate data security. Part of the interest and fees paid by Plaintiffs and Class Members to Nelnet were intended to be used to fund adequate data security. Plaintiffs and Class Members did not get what they paid for.

109. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Nelnet has failed to disclose when the breach occurred or how long it lasted, forcing customers to continue to monitor their accounts indefinitely.

110. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further

by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

111. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

112. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including Social Security numbers) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

113. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

VI. Defendants' Failure to Notify Plaintiffs and Class Members in a Timely or Adequate Fashion Exacerbated the Damages

114. As detailed above, Nelnet claims to have discovered the Data Breach on July 21, 2022 yet failed to even *begin* notifying Plaintiffs and Class Members on behalf of EdFinancial and OSLA until August 26, 2022 via U.S. Mail.

115. This period of over a month could have been used by Plaintiffs and Class Members to take steps to mitigate the damage caused by the Data Breach.

116. Instead, Nelnet concealed the Data Breach for over a month, allowing the unauthorized third-party to potentially exploit Plaintiffs' and Class Members' PII without any mitigation steps being taken.

117. Plaintiffs and Class Members were deprived of the opportunity to take any steps to prevent damage by Nelnet's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

VII. Plaintiffs' Allegations

a. Plaintiff Ian Scott

118. Plaintiff Ian Scott ("Plaintiff Scott") is a citizen and resident of the State of New Mexico.

119. Plaintiff Scott's student loans were assigned to EdFinancial without his consent or input.

120. EdFinancial and Nelnet required Plaintiff Scott to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

121. Plaintiff Scott was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

122. Plaintiff Scott's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach

123. As a result of the Data Breach, Plaintiff Scott spent time and effort researching the Data Breach, reviewing and monitoring his account for fraudulent activity, signing up for

credit monitoring services, and dealing with phishing attempts via email and telephone calls using the information taken in the Data Breach.

124. Plaintiff Scott places significant value in the security of his PII. Plaintiff Scott entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

125. Plaintiff Scott and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Scott and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

126. As a result of the Data Breach, Plaintiff Scott has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

b. Plaintiff Jessica Alexander

127. Plaintiff Jessica Alexander ("Plaintiff Alexander") is a citizen and resident of the State of California.

128. Plaintiff Alexander's student loans were assigned to EdFinancial without her consent or input.

129. EdFinancial and Nelnet required Plaintiff Alexander to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

130. Plaintiff Alexander was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

131. As a result of the Data Breach, Plaintiff Alexander spent time and effort researching the Data Breach, and reviewing and monitoring her account for fraudulent activity.

132. Plaintiff Alexander places significant value in the security of her PII. Plaintiff Alexander entrusted her PII to EdFinancial with the understanding that EdFinacial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

133. Plaintiff Alexander and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Alexander and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

134. As a result of the Data Breach, Plaintiff Alexander has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

c. Plaintiff Pamela Bump

135. Plaintiff Pamela Bump ("Plaintiff Bump") is a citizen and resident of the Commonwealth of Massachusetts.

136. Plaintiff Bump's student loans were assigned to EdFinancial without her consent or input.

137. EdFinancial and Nelnet required Plaintiff Bump to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

138. Plaintiff Bump was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

139. Plaintiff Bump's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

140. As a result of the Data Breach, Plaintiff Bump spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

141. Plaintiff Bump places significant value in the security of her PII. Plaintiff Bump entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

142. Plaintiff Bump and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Bump and Class

Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

143. As a result of the Data Breach, Plaintiff Bump has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

d. Plaintiff Bridget Cahill

144. Plaintiff Bridget Cahill ("Plaintiff Cahill") is a citizen and resident of the Commonwealth of Massachusetts.

145. Plaintiff Cahill's student loans were assigned to EdFinancial without her consent or input.

146. EdFinancial and Nelnet required Plaintiff Cahill to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

147. Plaintiff Cahill was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

148. Plaintiff Cahill's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

149. As a Result of the Data Breach, Plaintiff Cahill spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and signing up for credit monitoring services.

150. Plaintiff Cahill places significant value in the security of her PII. Plaintiff Cahill entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her

information secure and employ reasonable adequate security measures to ensure that it would not be compromised.

151. Plaintiff Cahill and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Cahill and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

152. As a result of the Data Breach, Plaintiff Cahill has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach

e. Plaintiff Lesly Canales

153. Plaintiff Lesly Canales ("Plaintiff Canales") is a citizen and resident of the State of New York.

154. Plaintiff Canales' student loans were assigned to EdFinancial without her consent or input.

155. EdFinancial and Nelnet required Plaintiff Canales to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

156. Plaintiff Canales was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

157. Plaintiff Canales's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

158. As a result of the Data Breach, Plaintiff Canales spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and signing up for credit monitoring services

159. Plaintiff Canales places significant value in the security of her PII. Plaintiff Canales entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

160. Plaintiff Canales and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Canales and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

161. As a result of the Data Breach, Plaintiff Canales has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

f. Plaintiff Melissa Charbonneau

162. Plaintiff Melissa Charbonneau ("Plaintiff Charbonneau") is a citizen and resident of the State of Illinois.

163. Plaintiff Charbonneau's student loans were assigned to EdFinancial without her consent or input.

164. EdFinancial and Nelnet required Plaintiff Charbonneau to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

165. Plaintiff Charbonneau was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

166. Plaintiff Charbonneau's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

167. As a result of the Data Breach, Plaintiff Charbonneau spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity signing up for credit monitoring services, setting up alerts through her credit card company, and signing up for identity theft services and alerts through Discover.

168. Plaintiff Charbonneau places significant value in the security of her PII. Plaintiff Charbonneau entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

169. Plaintiff Charbonneau and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Charbonneau

and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

170. As a result of the Data Breach, Plaintiff Charbonneau has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

g. Plaintiff Douglas Conley

171. Plaintiff Dougles Conley ("Plaintiff Conley") is a citizen and resident of the State of Arizona.

172. Plaintiff Conley's student loans were assigned to EdFinancial without his consent or input.

173. EdFinancial and Nelnet required Plaintiff Conley to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

174. Plaintiff Conley was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

175. Plaintiff Conley's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

176. As a result of the Data Breach, Plaintiff Conley spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

177. Plaintiff Conley places significant value in the security of her PII. Plaintiff Conley entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her

information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

178. Plaintiff Conley and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Conley and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

179. As a result of the Data Breach, Plaintiff Conley has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

h. Plaintiff Noah Helvey

180. Plaintiff Noah Helvey ("Plaintiff Helvey") is a citizen and resident of the State of Utah.

181. Plaintiff Helvey's student loans were assigned to EdFinancial without his consent or input.

182. EdFinancial and Nelnet required Plaintiff Helvey to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

183. Plaintiff Helvey was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

184. Plaintiff Helvey's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

185. As a result of the Data Breach, Plaintiff Helvey spent time and effort researching the Data Breach; reviewing and monitoring his accounts for fraudulent activity; signing up for credit monitoring services; dealing with phishing attempt via email, text, and telephone calls; dealing with notifications regarding someone trying to access her various accounts connected to the email used for EdFinancial; and configuring notifications for fraudulent activity on Credit Karma, Experian and Capital One

186. Plaintiff Helvey places significant value in the security of her PII. Plaintiff Helvey entrusted is PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

187. Plaintiff Helvey and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Helvey and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

188. As a result of the Data Breach, Plaintiff Helvey has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

i. Plaintiff Dallin Iller

189. Plaintiff Dallin Iler ("Plaintiff Iler") is a citizen and resident of the State of Indiana.

190. Plaintiff Iler's student loans were assigned to EdFinancial without his consent or input.

191. EdFinancial and Nelnet required Plaintiff Iler to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

192. Plaintiff Iler was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

193. Plaintiff Iler's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

194. As a result of the Data Breach, Plaintiff Iler spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity.

195. Plaintiff Iler places significant value in the security of his PII. Plaintiff Iler entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

196. Plaintiff Iler and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Iler and Class

Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

197. As a result of the Data Breach, Plaintiff Iler has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

j. Plaintiff Dustin Jones

198. Plaintiff Dustin Jones ("Plaintiff Jones") is a citizen and resident of the Commonwealth of Pennsylvania.

199. Plaintiff Jones' student loans were assigned to EdFinancial without his consent or input.

200. EdFinancial and Nelnet required Plaintiff Jones to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

201. Plaintiff Jones was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

202. Plaintiff Jones's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

203. As a result of the Data Breach, Plaintiff Jones spent time and effort researching the Data Breach; reviewing and monitoring his accounts for fraudulent activity; signing up credit monitoring services; freezing credit cards; dealing with phishing attempts via text, email, and telephone calls; and regularly reporting to identitytheft.gov.

204. Plaintiff Jones experienced three unauthorized hard credit inquiries from September 9, 2022 through September 11, 2022 which impacted his credit. As a result of these hard inquireies, Plaintiff Jones was forced to expend time and resources filing disputes with the three major credit bureaus and freeze his credit. Plaintiff Jones also filed a police report reporting the attempted identity theft.

205. Additionally, several attempts were made to open credit cards in Mr. jones' name, including a Target RedCard and a Capital One Plaitnum Credit Card using Plaintiff Jones' PII obtained in the Data Breach. As a result of these consequences, Plaintiff Jones purchased Experian IdentityWorks℠ Premium to monitor his credit.

206. Plaintiff Jones places significant value in the security of his PII. Plaintiff Jones entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

207. Plaintiff Jones and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Jones and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

208. As a result of the Data Breach, Plaintiff Jones has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to

come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach

k. Plaintiff Kayli Lazarz

209. Plaintiff Kayli Lazarz ("Plaintiff Lazarz") is a citizen and resident of the State of Colorado.

210. Plaintiff Lazarz's student loans were assigned to EdFinancial without her consent or input.

211. EdFinancial and Nelnet required Plaintiff Lazarz to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

212. Plaintiff Lazarz was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

213. Plaintiff Lazarz's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

214. As a result of the Data Breach, Plaintiff Lazarz spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

215. Plaintiff Lazarz places significant value in the security of her PII. Plaintiff Lazarz entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

216. Plaintiff Lazarz and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent

activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Lazarz and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

217. As a result of the Data Breach, Plaintiff Lazarz has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

l. Plaintiff Brittni Linn

218. Plaintiff Brittni Linn ("Plaintiff Linn") is a citizen and resident of the Commonwealth of Pennsylvania.

219. Plaintiff Linn's student loans were assigned to EdFinancial without her consent or input.

220. EdFinancial and Nelnet required Plaintiff Linn to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

221. Plaintiff Linn was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

222. Plaintiff Linn's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

223. As a result of the Data Breach, Plaintiff Linn spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

224. Plaintiff Linn places significant value in the security of her PII. Plaintiff Linn entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

225. Plaintiff Linn and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Linn and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

226. As a result of the Data Breach, Plaintiff Linn has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

m. Plaintiff Delilah Oliveira

227. Plaintiff Delilah Oliveira ("Plaintiff Oliveira") is a citizen and resident of the Commonwealth of Massachusetts.

228. Plaintiff Oliveria's student loans were assigned to EdFinancial without her consent or input.

229. EdFinancial and Nelnet required Plaintiff Oliveira to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

230. Plaintiff Oliveira was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

231. Plaintiff Oliveira's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

232. As a result of the Data Breach, Plaintiff Oliveira spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, calling the credit bureaus concerning credit freezes, dealing with an incident where a hacker tried using her credit card, replacing her credit cards, and changing passwords to several online accounts; she was not informed of the credit 24-month credit monitoring service offered by EdFinancial through Experian.

233. Plaintiff Oliveira places significant value in the security of her PII. Plaintiff Oliveira entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

234. Plaintiff Oliveira and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Oliveira and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

235. As a result of the Data Breach, Plaintiff Oliveira has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to

come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

n. Plaintiff Devinne Peterson

236. Plaintiff Devinne Peterson ("Plaintiff Peterson") is a citizen and resident of the Commonwealth of Pennsylvania.

237. Plaintiff Peterson's student loans were assigned to EdFinancial without her consent or input.

238. EdFinancial and Nelnet required Plaintiff Peterson to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

239. Plaintiff Peterson was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

240. Plaintiff Peterson's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

241. As a result of the Data Breach, Plaintiff Peterson spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity.

242. Plaintiff Peterson places significant value in the security of her PII. Plaintiff Peterson entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

243. Plaintiff Peterson and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent

activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Peterson and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

244. As a result of the Data Breach, Plaintiff Peterson has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

o. Plaintiff Eric Polanco

245. Plaintiff Eric Polanco ("Plaintiff Polanco") is a citizen and resident of the State of California.

246. Plaintiff Polanco's student loans were assigned to EdFinancial without his consent or input.

247. EdFinancial and Nelnet required Plaintiff Polanco to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

248. Plaintiff Polanco was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

249. Plaintiff Polanco's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

250. As a result of the Data Breach, Plaintiff Polanco spent time and effort researching the Data Breach and reviewing and monitoring is accounts for fraudulent activity.

251. Plaintiff Polanco places significant value in the security of his PII. Plaintiff Polanco entrusted her PII to EdFinancial with the understanding that EdFinancial would keep is information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

252. Plaintiff Peterson and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Polanco and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

253. As a result of the Data Breach, Plaintiff Polanco has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

p. Plaintiff Justin Randall

254. Plaintiff Justin Randall ("Plaintiff Randall") is a citizen and resident of the State of Wisconsin.

255. Plaintiff Randall's student loans were assigned to EdFinancial without his consent or input.

256. EdFinancial and Nelnet required Plaintiff Randall to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

257. Plaintiff Randall was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

258. Plaintiff Randall's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

259. As a result of the Data Breach, Plaintiff Randall spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity.

260. Plaintiff Randall places significant value in the security of his PII. Plaintiff Randall entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

261. Plaintiff Randall and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Randall and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

262. As a result of the Data Breach, Plaintiff Randall has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

q. Plaintiff Sofia Rodriguez

263. Plaintiff Sofia Rodriguez ("Plaintiff Rodriguez") is a citizen and resident of the State of Michigan.

264. Plaintiff Rodriguez's student loans were assigned to EdFinancial without her consent or input.

265. EdFinancial and Nelnet required Plaintiff Rodriguez to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

266. Plaintiff Rodriguez was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

267. Plaintiff Rodriguez's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

268. As a result of the Data Breach, Plaintiff Rodriguez spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and monitoring her credit several times each month.

269. Plaintiff Rodriguez places significant value in the security of her PII. Plaintiff Rodriguez entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

270. Plaintiff Rodriguez and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of

their personal information, and other economic and non-economic harm. Plaintiff Rodriguez and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

271. As a result of the Data Breach, Plaintiff Rodriguez has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

r. Plaintiff Josh Sanchez

272. Plaintiff Josh Sanchez ("Plaintiff Sanchez") is a citizen and resident of the State of Florida.

273. Plaintiff Sanchez's student loans were assigned to EdFinancial without his consent or input.

274. EdFinancial and Nelnet required Plaintiff Sanchez to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

275. Plaintiff Sanchez was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

276. Plaintiff Sanchez's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

277. As a result of the Data Breach, Plaintiff Sanchez spent time and effort researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, signing up for credit monitoring services, and reaching out to Venmo support due to being notified of someone making several unsuccessful attempts to log in

278. Plaintiff Sanchez places significant value in the security of his PII. Plaintiff Sanchez entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

279. Plaintiff Sanchez and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Sanchez and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

280. As a result of the Data Breach, Plaintiff Sanchez has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

s. Plaintiff Charles Sangmeister

281. Plaintiff Charles Sangmeister ("Plaintiff Sangmeister") is a citizen and resident of the State of California.

282. Plaintiff Sangmeister's student loans were assigned to EdFinancial without her consent or input.

283. EdFinancial and Nelnet required Plaintiff Sangmeister to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

284. Plaintiff Sangmeister was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

285. Plaintiff Sangmeister's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

286. As a result of the Data Breach, Plaintiff Sangmeister spent time and effort researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and dealing with phishing attempts via text and email, and spam marketing calls to his home phone lines.

287. Plaintiff Sangmeister places significant value in the security of his PII. Plaintiff Sangmeister entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

288. Plaintiff Sangmeister and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Sangmeister and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

289. As a result of the Data Breach, Plaintiff Sangmeister has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

t. Plaintiff William Spearman

290. Plaintiff William Spearman ("Plaintiff Spearman") is a citizen and resident of the State of South Carolina.

291. Plaintiff Spearman's student loans were assigned to EdFinancial without his consent or input.

292. EdFinancial and Nelnet required Plaintiff Spearman to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

293. Plaintiff Spearman was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

294. Plaintiff Spearman's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

295. As a result of the Data Breach, Plaintiff Spearman spent time and effort researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, changing passwords, auditing the security of his home network and personal devices, dealing with an increase in phishing attempts via telephone calls and emails, spending $800 on a commercial grade firewall for his home network, and purchasing a monthly subscription to a VPN service.

296. Plaintiff Spearman places significant value in the security of his PII. Plaintiff Spearman entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

297. Plaintiff Spearman and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Spearman and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

298. As a result of the Data Breach, Plaintiff Spearman has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.Incident" notifying Plaintiff Spearman that his PII was compromised in the Data Breach.

u. Plaintiff Taylor Vetter

299. Plaintiff Taylor Vetter ("Plaintiff Vetter") is a citizen and resident of the State of New York.

300. Plaintiff Vetter's student loans were assigned to EdFinancial without her consent or input.

301. EdFinancial and Nelnet required Plaintiff Vetter to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

302. Plaintiff Vetter was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

303. Plaintiff Vetter's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

304. As a result of the Data Breach, Plaintiff Vetter spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

305. Plaintiff Vetter places significant value in the security of her PII. Plaintiff Vetter entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

306. Plaintiff Vetter and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff Vetter and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

307. As a result of the Data Breach, Plaintiff Vetter has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

v. Plaintiff Rachel Woods

308. Plaintiff Rachel Woods ("Plaintiff Woods") is a citizen and resident of the State of Texas.

309. Plaintiff Woods' student loans were assigned to EdFinancial without her consent or input.

310. EdFinancial and Nelnet required Plaintiff Woods to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

311. Plaintiff Woods was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

312. Plaintiff Woods's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

313. As a result of the Data Breach, Plaintiff Woods spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

314. Plaintiff Woods places significant value in the security of her PII. Plaintiff Woods entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

315. Plaintiff Woods and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Woods and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

316. As a result of the Data Breach, Plaintiff Woods has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

w. Plaintiff Garner J. Kohrell

317. Plaintiff Garner J. Kohrell ("Plaintiff Kohrell") is a citizen and resident of the State of Minnesota.

318. Plaintiff Kohrell's student loans were assigned to EdFinancial without his consent or input.

319. EdFinancial and Nelnet required Plaintiff Kohrell to provide his PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

320. Plaintiff Kohrell was notified of the Data Breach and the impact to his PII by EdFinancial via U.S. Mail.

321. Plaintiff Kohrell's PII was disclosed without his authorization to unknown third parties as a result of the Data Breach.

322. As a result of the Data Breach, Plaintiff Kohrell spent time and effort researching the Data Breach and reviewing and monitoring his accounts for fraudulent activity.

323. Plaintiff Kohrell places significant value in the security of his PII. Plaintiff Kohrell entrusted his PII to EdFinancial with the understanding that EdFinancial would keep his information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

324. Plaintiff Kohrell and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of his personal information, and other economic and non-economic harm. Plaintiff Kohrell and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

325. As a result of the Data Breach, Plaintiff Kohrell has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

x. Plaintiff Olivia Covington

326. Plaintiff Olivia Covington ("Plaintiff Covington") is a citizen and resident of the Commonwealth of Virginia.

327. Plaintiff Covington's student loans were assigned to EdFinancial without her consent or input.

328. EdFinancial and Nelnet required Plaintiff Covington to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

329. Plaintiff Covington was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

330. Plaintiff Covington'ss PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

331. As a result of the Data Breach, Plaintiff Covington spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and responding to fraudulently opened credit card accounts. For example, on July 31, 2022, Plaintiff Covington discovered that a credit card account with Capital One had been opened in her name using her information stolen in the Data Breach. Plaintiff Covington did not open this account and suffered harm in the form of impact to her credit score, among other things, from the unauthorized opening of this Capital One credit card account.

332. Plaintiff Covington places significant value in the security of her PII. Plaintiff Covington entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

333. Plaintiff Covington and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Covington and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

334. As a result of the Data Breach, Plaintiff Covington has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

y. Plaintiff Alexis Luna

335. Plaintiff Alexis Luna ("Plaintiff Luna") is a citizen and resident of the State of California.

336. Plaintiff Luna's student loans were assigned to EdFinancial without her consent or input.

337. EdFinancial and Nelnet required Plaintiff Luna to provide her PII to EdFinancial and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by EdFinancial and Nelnet.

338. Plaintiff Luna was notified of the Data Breach and the impact to her PII by EdFinancial via U.S. Mail.

339. Plaintiff Luna'ss PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

340. As a result of the Data Breach, Plaintiff Luna spent time and effort researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and responding to alerts regarding fraudulently activity associated with her credit. For example, after the Data Breach occurred, Plaintiff Luna has had 7 unauthorized inquiries on her credit, and her personal information associated with her social security number on file with Experian was changed without her consent.

341. Plaintiff Luna places significant value in the security of her PII. Plaintiff Luna entrusted her PII to EdFinancial with the understanding that EdFinancial would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

342. Plaintiff Luna and Class Members suffered actual damages as a result of the failures of EdFinancial and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Luna and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

343. As a result of the Data Breach, Plaintiff Luna has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

z. Plaintiff Mary Traynor

344. Plaintiff Mary Traynor ("Plaintiff Traynor") is a citizen and resident of the State of Illinois.

345. Plaintiff Traynor's student loans were assigned to OSLA without her consent or input.

346. OSLA and Nelnet required Plaintiff Traynor to provide her PII to OSLA and Nelnet in order to create an account and make loan payments electronically via the web payment portal services provided by OSLA and Nelnet.

347. Plaintiff Traynor was notified of the Data Breach and the impact to her PII by OSLA via U.S. Mail.

348. Plaintiff Traynor's PII was disclosed without her authorization to unknown third parties as a result of the Data Breach.

349. As a result of the Data Breach, Plaintiff Traynor spent time and effort researching the Data Breach and reviewing and monitoring her accounts for fraudulent activity.

350. Plaintiff Traynor places significant value in the security of her PII. Plaintiff Traynor entrusted her PII to OSLA with the understanding that OSLA would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

351. Plaintiff Traynor and Class Members suffered actual damages as a result of the failures of OSLA and Nelnet to adequately protect the sensitive information entrusted to them, including, without limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff Traynor and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identify theft.

352. As a result of the Data Breach, Plaintiff Traynor has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

CLASS ACTION ALLEGATIONS

353. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Nationwide Class").

354. Plaintiffs reserve the right to modify, expand or amend the above Nationwide Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

ARIZONA SUBCLASS

355. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Arizona Subclass:

> All persons in Arizona whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Arizona Subclass").

356. Plaintiffs reserve the right to modify, expand or amend the above Arizona Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

CALIFORNIA SUBCLASS

357. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

> All persons in California whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "California Subclass").

358. Plaintiffs reserve the right to modify, expand or amend the above California Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

COLORDAO SUBCLASS

359. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

> All persons in Colorado whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Colorado Subclass").

360. Plaintiffs reserve the right to modify, expand or amend the above Colorado Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

FLORIDA SUBCLASS

361. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Florida Subclass:

> All persons in Florida whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Florida Subclass").

362. Plaintiffs reserve the right to modify, expand or amend the above Florida Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

ILLINOIS SUBCLASS

363. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Illinois Subclass:

> All persons in Illinois whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Illinois Subclass").

364. Plaintiffs reserve the right to modify, expand or amend the above Illinois Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

INDIANA SUBCLASS

365. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Indiana Subclass:

> All persons in Indiana whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Indiana Subclass").

366. Plaintiffs reserve the right to modify, expand or amend the above Indiana Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MASSACHUSETTS SUBCLASS

367. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Massachusetts Subclass:

> All persons in Massachusetts whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Massachusetts Subclass").

368. Plaintiffs reserve the right to modify, expand or amend the above Massachusetts Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MICHIGAN SUBCLASS

369. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Michigan Subclass:

> All persons in Michigan whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Michigan Subclass").

370. Plaintiffs reserve the right to modify, expand or amend the above Michigan Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

NEW MEXICO SUBCLASS

371. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following New Mexico Subclass:

> All persons in New Mexico whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "New Mexico Subclass").

372. Plaintiffs reserve the right to modify, expand or amend the above New Mexico Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

NEW YORK SUBCLASS

373. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following New York Subclass:

> All persons in New York whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "New York Subclass").

374. Plaintiffs reserve the right to modify, expand or amend the above New York Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

PENNSYLVANIA SUBCLASS

375. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Pennsylvania Subclass:

> All persons in Pennsylvania whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Pennsylvania Subclass").

376. Plaintiffs reserve the right to modify, expand or amend the above Pennsylvania Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

SOUTH CAROLINA SUBCLASS

377. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following South Carolina Subclass:

> All persons in South Carolina whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "South Carolina Subclass").

378. Plaintiffs reserve the right to modify, expand or amend the above South Carolina Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

TEXAS SUBCLASS

379. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Texas Subclass:

> All persons in Texas whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Texas Subclass").

380. Plaintiffs reserve the right to modify, expand or amend the above Texas Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

UTAH SUBCLASS

381. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Utah Subclass:

> All persons in Utah whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Utah Subclass").

382. Plaintiffs reserve the right to modify, expand or amend the above Utah Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

WISCONSIN SUBCLASS

383. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Wisconsin Subclass:

> All persons in Wisconsin whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Wisconsin Subclass").[7]

[7] Collectively, the Arizona Subclass, California Subclass, Colorado Subclass, Florida Subclass, Illinois Subclass, Indiana Subclass, Massachusetts Subclass, Michigan Subclass, New Mexico Subclass, New York Subclass,

384. Plaintiffs reserve the right to modify, expand or amend the above Wisconsin Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

MINNESOTA SUBCLASS

385. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Minnesota Subclass:

> All persons in Minnesota whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Minnesota Subclass").

386. Plaintiffs reserve the right to modify, expand or amend the above Minnesota Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

VIRGINIA SUBCLASS

387. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Virginia Subclass:

> All persons in Virginia whose personal information was compromised in the Data Breach made public by Nelnet in August 2022 (the "Virginia Subclass").

388. Plaintiffs reserve the right to modify, expand or amend the above Virginia Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

389. Certification of Plaintiffs' claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements

---

Pennsylvania Subclass, South Carolina Subclass, Texas Subclass, Utah Subclass, Wisconsin Subclass, Minnesota Subclass, and Virginia are the "State Subclasses."

of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

390. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Nationwide Class and the State Subclasses are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While Plaintiffs are informed and believe that there are likely millions of Members of the Classes, the precise number of Class Members is unknown to Plaintiffs. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

391. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendants engaged in active misfeasance and misconduct alleged herein;

b. Whether Defendants owed a duty to Class Members to safeguard their sensitive personal information;

c. Whether Defendants breached its duty to Class Members to safeguard their sensitive personal information;

d. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Defendants' failure to provide adequate security proximately caused Plaintiffs' and Class Members' injuries; and

g. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

392. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of all Class and Subclass Members because Plaintiffs, like other Class and Subclass Members, suffered theft of their sensitive personal information in the Data Breach.

393. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are Members of the Classes and State Subclasses and their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intends to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

394. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

395. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants have acted, or refused to act, on grounds generally applicable to the Nationwide Class and Subclasses such that final declaratory or injunctive relief is appropriate.

396. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on newly learned facts or legal developments that arise following additional investigation, discovery, or otherwise.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

397. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

398. Nelnet, as the servicing system and customer website portal provider for loan servicers EdFinancial, obtained Plaintiffs' and Class Members' PII from Plaintiffs and Class

Members and/or EdFinancial. In turn, EdFinancial obtained PII from Plaintiffs and Class Members.

399. By collecting and maintaining sensitive personal information, Defendants had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Defendants' duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

400. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

401. Defendants' duty of care arose as a result of, among other things, the special relationship that existed between Defendants and its student loan borrowers it services. Nelnet, and EdFinancial who entrusted Plaintiffs' and Class Members' PII with them, were the only parties in a position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur that would result in substantial harm to consumers.

402. Defendants were subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Defendants.

403. Defendants breached its duties, and thus was negligent, by failing to use reasonable measures to protect customers' sensitive personal information. Defendants' negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against malware;

b. failure to comply with industry standards for software and server security;

c. failure to track and monitor access to its network and personal information;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to remove, delete, or destroy highly sensitive personal information of consumers that is no longer being used for any valid business purpose;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing personal information from its network while the Data Breach was taking place.

i. failure to oversee the entrustment of student loan borrowers' PII

404. It was foreseeable to Defendants that a failure to use reasonable measures to protect its customers' sensitive personal information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendants given the known frequency of data breaches and various warnings from industry experts.

405. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

406. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

407. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

408. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

409. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

410. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

411. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

412. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

413. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

414. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

415. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

416. When Plaintiffs and Class Members provided their sensitive personal information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants under which Defendants agreed to take reasonable steps to protect their sensitive personal information.

417. Defendants solicited and invited Plaintiffs and Class Members to provide their sensitive personal information as part of their regular business practices. Indeed, to sign up for a Nelnet account—which is required to make payments online to loan serviced by companies that hire Nelnet for web portal and payment processing services—Nelnet requires customers to provide sensitive personal information including Social Security numbers, to obtain Nelnet's services. Plaintiffs and Class Members accepted Nelnet's offers and provided their sensitive personal information Nelnet.

418. Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards when they entered into the implied contracts with Nelnet.

419. Plaintiffs and Class Members paid money (directly and/or indirectly) to Defendants and Plaintiffs and Class Members therefore reasonably believed and expected that Defendants would use part of those funds to obtain and oversee adequate data security. Defendants failed to do so.

420. Plaintiffs and Class Members would not have provided their sensitive personal information to Defendants in the absence of Defendants' implied promise to keep their sensitive personal information reasonably secure.

421. Plaintiffs and Class Members fully performed their obligations under the implied contracts by paying money to Defendants.

422. Defendants breached its implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures.

423. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

424. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

425. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

426. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of monies paid while utilizing Defendants' online services.

427. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendants also benefited from the receipt of Plaintiffs' and Class Members' sensitive personal information as this was utilized by Defendants to send bills and process payments for services, among other things.

428. The monies Plaintiffs and Class Members paid to Defendants were supposed to be used by Defendants, in part, to pay for and oversee adequate data privacy infrastructure, practices, and procedures.

429. Defendants' conduct caused Plaintiffs and Class Members to suffer actual damages in an amount equal to the difference in value between what they paid for (Defendants' services made with adequate data privacy and security practices and procedures), and what they actually received (Defendants' services without adequate data privacy and security practices and procedures).

430. In equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to oversee, implement, or adequately implement, the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

431. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF CONFIDENCE
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

432. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

433. Plaintiffs and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose to unauthorized parties the PII provided by Plaintiffs and Class Members to Defendants to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

434. Defendants knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII they collected, stored, and maintained.

435. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the PII in its possession and failed to comply with industry-standard data security practices.

436. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

437. But for Defendants' disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.The injury and harm Plaintiffs and Class Members suffered was the reasonably

foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendants knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and members of the Class' PII had serious security vulnerabilities because Defendants failed to observe even basic information security practices or correct known security vulnerabilities.

438. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and members of the Class have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT VI
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

439. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

440. Plaintiffs shared PII with Defendants that Plaintiffs wanted to remain private and non-public.

441. Plaintiffs reasonably expected that the PII they shared with Defendants would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

442. Defendants intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

443. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

444. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other PII.

445. Defendants' intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

446. As a direct and proximate result of Defendants' invasions of privacy, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost value of access to their PII permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT VII
ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *et seq.*
(On behalf of Plaintiff Conley and the Arizona Subclass)

447. Plaintiff Conley individually and on behalf of the Arizona Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

448. Defendants are each a "person" as defined by A.R.S. § 44-1521(6).

449. Defendants advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

450. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

451. Defendants' unfair and deceptive acts and practices included:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Conley's and Arizona Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Conley's and Arizona Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Conley's and Arizona Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Conley's and Arizona Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

452. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

453. Defendants intended to mislead Plaintiffs and Arizona Subclass Members and induce them to rely on its misrepresentations and omissions.

454. Had Defendants disclosed to Plaintiff Conley and Arizona Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defemdamts would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable PII

regarding millions of consumers, including Plaintiff Conley and the Arizona Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Conley and the Arizona Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

455. Defendants acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff Conley's and Arizona Subclass Members' rights.

456. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff Conley and Arizona Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

457. Plaintiff Conley and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT VIII
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code §§ 1798.150, *et seq.*
(On behalf of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and the California Subclass)

458. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna individually and on behalf of the California Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

459. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass members are residents of California.

460. Upon information and belief Defendants are each a business under Cal. Civ. Code § 1798.140(d).

461. Defendants collect consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

462. Defendants violated § 1798.150 of the CCPA by failing to protect Plaintiff Alexander, Plaintiff Sangmeister. Plaintiff Polanco, and Plaintiff Luna's and California Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

463. Defendants has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna's and California Subclass Members' PII. As detailed herein, Defendants failed to do so.

464. As a direct and proximate result of Defendants' acts, the PII of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass

Members, including social security numbers, phone numbers, names, addresses, and email addresses, was subjected to unauthorized access and exfiltration, theft, or disclosure.

465. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and California Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold customers' PII, including Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Members' PII. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Defendants has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

466. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

467. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants and third parties with similar inadequate security measures.

468. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and the California Subclass seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

COUNT IX
CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq.*
(On behalf of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and the California Subclass)

469. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna individually and on behalf of the California Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

470. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and California Subclass Members are residents of California.

471. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

472. Defendants are each a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Subclass Members.

473. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the

types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

474. Defendants are each a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

475. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

476. Because Defendants reasonably believed that Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII was acquired by unauthorized persons during the Defendants' Data Breach, Defendants had an obligation to disclose the Nelnet Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

477. Defendants failed to fully disclose material information about the Data Breach, including the types of PII impacted, in a timely fashion.

478. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

479. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass members suffered damages, as described above.

480. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT X
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On behalf of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco and the California Subclass)

481. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna individually and on behalf of the California Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

482. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and California Subclass members are residents of California.

483. Defendants are each "person" as defined by Cal. Bus. & Prof. Code §17201.

484. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

485. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna's and California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna's and California Subclass Members, whose PII has been compromised.

c. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Defendants' failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' grossly inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

486. Defendants engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

487. Defendants has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

488. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and

Plaintiff Luna's and California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna's and California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, and 1798.81.5, which was a direct and proximate cause of the Data Breach.

489. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

490. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

491. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna's and California Subclass Members' rights. Defendants'

numerous past data breaches put it on notice that its security and privacy protections were inadequate.

492. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT XI
VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750, *et seq.*
(On behalf of Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and the California Subclass)

493. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, and Plaintiff Luna individually and on behalf of the California Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

494. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass members are residents of California.

495. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

496. Defendants are each a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

497. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

498. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna and California Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

499. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

500. Had Defendants disclosed to Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and California Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants were trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and the California Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff

Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and the California Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

501. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and the California Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

502. Plaintiff Alexander, Plaintiff Sangmeister, Plaintiff Polanco, Plaintiff Luna, and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT XII
COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat. §§ 6-1-716, *et seq.*
(On behalf of Plaintiff Lazarz and the Colorado Subclass)

503. Plaintiff Lazarz individually and on behalf of the Colorado Subclass, repeats and realleges all allegations as if fully set forth herein.

504. Defendants are each a business that owns or licenses computerized data that includes PII as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

505. The PII of Plaintiff Lazarz and the Colorado Subclass (*e.g.*, Social Security numbers) includes PII as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

506. Defendants is required to accurately notify Plaintiff Lazarz and the Colorado Subclass if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

507. Because Defendants was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

508. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Colo. Rev. Stat. § 6-1-716(2).

509. As a direct and proximate result of Defendants' violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff Lazarz and Colorado Subclass Members suffered damages, as described above.

510. Plaintiff Lazarz and the Colorado Subclass Members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT XIII
COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq.*
(On behalf of Plaintiff Lazarz and the Colorado Subclass)

511. Plaintiff Lazarz individually and on behalf of the Colorado Subclass, repeats and realleges all allegations as if fully set forth herein.

512. Defendants are each a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

513. Defendants engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

514. Plaintiff Lazarz and Colorado Subclass Members, as well as the general public, are actual or potential consumers of the products and services offered by Defendants or successors in interest to actual consumers.

515. Defendants engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Defendants knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised;

d. Employing "bait and switch" advertising, which is advertising accompanied by an effort to sell goods, services, or property other than those advertised or on terms other than those advertised; and

e. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

516. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Lazarz's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Lazarz's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Lazarz's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Lazarz's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Lazarz and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Lazarz's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

517. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

518. Defendants intended to mislead Plaintiff Lazarz and Colorado Subclass Members and induce them to rely on its misrepresentations and omissions.

519. Had Defendants disclosed to Plaintiff Lazarz and the Colorado Subclass that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Lazarz and the Colorado Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Lazarz and the Colorado Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

520. Defendants acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff Lazarz's and Colorado Subclass Members' rights. Defendants' numerous past data breaches put it on notice that its security and privacy protections were inadequate.

521. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff Lazarz and the Colorado Subclass suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII, monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

522. Defendants' deceptive trade practices significantly impact the public, because many Members of the public are actual or potential consumers of Defendants' services and the Data Breach affected millions of Americans, which include Members of the Colorado Subclass.

523. Plaintiff Lazarz and the Colorado Subclass seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XIV
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, *et seq.*
(On behalf of Plaintiff Sanchez and the Florida Subclass)

524. Plaintiff Sanchez, individually and on behalf of the Florida Subclass, repeats and realleges the allegations above as if fully set forth herein.

525. Plaintiff Sanchez and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

526. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

527. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Sanchez's and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Sanchez's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Sanchez's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Sanchez's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Sanchez's and Florida Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Sanchez's and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2).

528. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

529. Had Defendants disclosed to Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and the Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

530. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff Sanchez and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

531. Plaintiff Sanchez and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages under Fla. Stat. § 501.211; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

COUNT XV
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815l. Comp. Stat. §§ 510/2, *et seq.*
(On behalf of Plaintiff Charbonneau, Plaintiff Traynor, and the Illinois Subclass)

532. Plaintiff Charbonneau, individually and on behalf of the Illinois Subclass, repeats and realleges all preceding allegations as if fully set forth herein.

533. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

534. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

535. Defendants' deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Charbonneau's and Illinois Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Charbonneau's and Illinois Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Charbonneau's and Illinois Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Charbonneau's and Illinois Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, Illinois

laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

536. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

537. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Charbonneau and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

538. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff Charbonneau and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

539. Plaintiff Charbonneau and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT XVI
INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code §§ 24-5-0.5-1, *et seq.*
(On behalf of Plaintiff Iler and the Indiana Subclass)

540. Plaintiff Iler individually and on behalf of the Indiana Subclass, repeats and realleges all allegations as if fully set forth herein.

541. Defendants are each a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

542. Defendants is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

543. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

544. Defendants' representations and omissions include both implicit and explicit representations, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Iler's and Indiana Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Iler's and Indiana Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Iler's and Indiana Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Iler's and Indiana Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

545. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

546. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

547. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

548. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

549. Defendants' acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendants' failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendants' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Defendants concerning the state of Defendants security, and because it is functionally impossible

for consumers to obtain credit without their PII being in Defendants' systems.

d. Because Defendants took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

550. Defendants also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

551. Defendants intended to mislead Plaintiff Iler and Indiana Subclass Members and induce them to rely on its misrepresentations and omissions.

552. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

553. Had Defendants disclosed to Plaintiff Iler and Indiana Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable

to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Iler and the Indiana Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Iler and Indiana Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

554. Defendants had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendants and Plaintiff Iler and the Indiana Subclass as described herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff Iler and the Indiana Subclass-and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff Iler and the Indiana Subclass that contradicted these representations.

555. Defendants acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff Iler's and Indiana Subclass Members' rights. Defendants' actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

556. Defendants' conduct includes incurable deceptive acts that Defendants engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8). As a direct and proximate result of Defendants' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff Iler and Indiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

557. Defendants' violations present a continuing risk to Plaintiff Iler and Indiana Subclass Members as well as to the public.

558. Plaintiff Iler and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT XVII
MASSACHUSETTS CONSUMER PROTECTION ACT
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*
(On behalf of Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and the Massachusetts Subclass)

559. Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco individually and on behalf of the Massachusetts Subclass repeats and realleges all allegations as if fully set forth herein.

560. Defendants and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

561. Defendants operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

562. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

563. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of

cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

564. Defendants' acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendants solely held the true facts about its inadequate security for PII, which Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira, Plaintiff Polanco and the Massachusetts Subclass could not independently discover.

565. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

566. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

567. Defendants intended to mislead Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira, Plaintiff Polanco and the Massachusetts Subclass and induce them to rely on its misrepresentations and omissions. Defendants' representations and omissions were material

because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

568. Defendants acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira and Plaintiff Polanco's and Massachusetts Subclass Members' rights.

569. As a direct and proximate result of Defendants' unfair and deceptive conduct, Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira, Plaintiff Polanco and the Massachusetts Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

570. Plaintiff Bump, Plaintiff Cahill, Plaintiff Oliveira, Plaintiff Polanco and the Massachusetts Subclass seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XVIII
MICHIGAN IDENTITY THEFT PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.72, *et seq.*
(On behalf of Plaintiff Rodriguez and the Michigan Subclass)

571. Plaintiff Rodriguez individually, and on behalf of the Michigan Subclass, repeats and realleges all allegations as if fully set forth herein.

572. Defendants is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

573. Plaintiff Rodriguez's and Michigan Subclass Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

574. Defendants is required to accurately notify Plaintiff Rodriguez and Michigan Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

575. Because Defendants discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

576. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Mich. Comp. Laws Ann. § 445.72(4).

577. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff Rodriguez and Michigan Subclass Members suffered damages, as described above.

578. Plaintiff Rodriguez and Michigan Subclass Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT XIX
MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.903, *et seq.*
(On behalf of Plaintiff Rodriguez and the Michigan Subclass)

579. Plaintiff Rodriguez individually, and on behalf of the Michigan Subclass, repeats and realleges all allegations as if fully set forth herein.

580. Defendants and Michigan Subclass Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

581. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

582. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter.

583. Defendants' unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Rodriguez's and Michigan Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Rodriguez's and Michigan Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez's and Michigan Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rodriguez's and Michigan Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rodriguez's and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

584. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

585. Defendants intended to mislead Plaintiff Rodriguez and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

586. Defendants acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff Rodriguez and Michigan Subclass Members' rights.

587. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive practices, Plaintiff Rodriguez and Michigan Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

588. Plaintiff Rodriguez and the Michigan Subclass seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

COUNT XX
NEW MEXICO UNFAIR PRACTICES ACT
N.M. Stat. Ann. §§ 57-12-2, *et seq*.
(On behalf of Plaintiff Scott and the New Mexico Subclass)

589. Plaintiff Scott individually and on behalf of the New Mexico Subclass, repeats and realleges the allegations above as if fully set forth herein.

590. Defendants are each a "person" as meant by N.M. Stat. Ann. § 57-12-2.

591. Defendants was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

592. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

593. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce in violation of N.M. Stat. § 57-12-2, including the following:

a. Representing that its goods and services have approval, characteristics, benefits, or qualities that they do not have;

b. Representing that its goods and services are of a particular standard or quality when they are of another;

c. Using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive;

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff Scott's and the New Mexico Subclass' detriment;

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff Scott and the New Mexico Subclass and the price paid, to their detriment.

594. Defendants' unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Scott's and New Mexico Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scott's and New Mexico Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Scott's and New Mexico Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scott's and New Mexico Subclass Members' PII, including duties imposed by the FTC Act, 15

U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Scott's and New Mexico Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Scott's and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

595. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

596. Defendants intended to mislead Plaintiff and New Mexico Subclass Members and induce them to rely on its misrepresentations and omissions.

597. Defendants acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff Scott's and New Mexico Subclass Members' rights. Defendants' numerous past data breaches put it on notice that its security and privacy protections were inadequate.

598. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable trade practices, Plaintiff Scott and New Mexico Subclass Members have suffered

and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

599. Plaintiff Scott and New Mexico Subclass Members seek all monetary and non-monetary relief allowed by law, including pursuant to N.M. Stat. Ann. § 57-12-10, injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

COUNT XXI
NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq.*
(On behalf of Plaintiff Canales, Plaintiff Vetter and the New York Subclass)

600. Plaintiff Canales and Plaintiff Vetter individually, and on behalf of the New York Subclass, repeats and realleges all allegations as if fully set forth herein.

601. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing

the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Canales and Plaintiff Vetter's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

602. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

603. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff Canales and Plaintiff Vetter's and New York Subclass Members' rights.

604. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff Canales, Plaintiff Vetter and the New York Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

605. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

606. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff Canales, Plaintiff Vetter and the New York Subclass that they could not reasonably avoid.

607. Plaintiff Canales, Plaintiff Vetter and the New York Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs

COUNT XXII
PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*
(On behalf of Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass)

608. Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson individually, and on behalf of the Pennsylvania Subclass, repeats and realleges all allegations as if fully set forth herein.

609. Defendants are each a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

610. Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

611. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

612. Defendants' unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and

Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

613. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

614. Defendants intended to mislead Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and Pennsylvania Subclass Members and induce them to rely on its misrepresentations and omissions.

615. Had Defendants disclosed to Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

616. Defendants acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and Pennsylvania Subclass Members' rights.

617. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff Jones, Plaintiff Linn and Plaintiff Peterson's and the Pennsylvania Subclass' reliance on them, Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

618. Plaintiff Jones, Plaintiff Linn, Plaintiff Peterson and the Pennsylvania Subclass seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT XXIII
SOUTH CAROLINA DATA BREACH SECURITY ACT
S.C. Code Ann. §§ 39-1-90, *et seq.*
(On behalf of Plaintiff Spearman and the South Carolina Subclass)

619. Plaintiff Spearman individually, and on behalf of the South Carolina Subclass, repeats and realleges all allegations if fully set forth herein.

620. Defendants is a business that owns or licenses computerized data or other data that includes personal identifying information (for the purpose of this count, "PII"), as defined by S.C. Code Ann. § 39-1-90(A).

621. Plaintiff Spearman's and South Carolina Subclass Members' PII (*e.g.,* Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

622. Defendants is required to accurately notify Plaintiff Spearman and South Carolina Subclass Members following discovery or notification of a breach of its data security system if PII that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

623. Because Defendants discovered a breach of its data security system in which PII that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

624. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated S.C. Code Ann. § 39-1-90(A).

625. As a direct and proximate result of Defendants' violations of S.C. Code Ann. § 39-1-90(A), Plaintiff Spearman and South Carolina Subclass Members suffered damages, as described above.

626. Plaintiff Spearman and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT XXIV
SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT
S.C. Code Ann. §§ 39-5-10, *et seq.*
(On behalf of Plaintiff Spearman and the South Carolina Subclass)

627. Plaintiff Spearman individually, and on behalf of the South Carolina Subclass, repeats and realleges all allegations if fully set forth herein.

628. Defendants are each a "person," as defined by S.C. Code Ann. § 39-5-10(a).

629. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

630. Defendants advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

631. Defendants engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Spearman's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Spearman's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Spearman's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Spearman's and South Carolina Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Spearman's and South Carolina Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Spearman's and South Carolina Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

632. Defendants' acts and practices had, and continue to have, the tendency or capacity to deceive.

633. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

634. Defendants intended to mislead Plaintiff Spearman and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

635. Had Defendants disclosed to Plaintiff Spearman and the South Carolina Subclass that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been

unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Spearman and the South Carolina Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Spearman and the South Carolina Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

636. Defendants had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff Spearman and the South Carolina Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to the PII in Defendants' possession and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the South Carolina Subclass that contradicted these representations.

637. Defendants' business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Defendants' acts and practices offend established public

policies that seek to protect consumers' PII and ensure that entities entrusted with PII use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq.*

638. Defendants' failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive given the sensitivity and extensivity of PII in its possession; its special role as a linchpin of the financial system; and its admitted duty of trustworthiness and care as an entrusted protector of data.

639. Defendants' unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Defendants engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including many South Carolinians impacted by the Data Breach.

640. Defendants' unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Defendants' policies and procedures, such as its security practices, create the potential for recurrence of the complained of business acts and practices.

641. Defendants' violations present a continuing risk to Plaintiffs and South Carolina Subclass Members as well as to the general public.

642. Defendants intended to mislead Plaintiff Spearman and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

643. Defendants acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff Spearman and South Carolina Subclass Members' rights. Defendants' numerous past data breaches put it on notice

that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Defendants and others from committing similar conduct in the future.

644. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiff Spearman and South Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

645. Plaintiff Spearman and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XXV
TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT
Texas Bus. & Com. Code §§ 17.41, *et seq.*
(On behalf of Plaintiff Woods and the Texas Subclass)

646. Plaintiff Woods individually, and on behalf of the Texas Subclass, repeats and realleges all allegations if fully set forth herein.

647. Defendants are each a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

648. Plaintiff Woods and Texas Subclass Members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

649. Defendants advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

650. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have approval, characteristics, uses, or benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised;

d. Failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed.

651. Defendants' false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Woods' and Texas Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Woods' and Texas Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Woods' and Texas Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Woods' and Texas Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

652. Defendants intended to mislead Plaintiff Woods and Texas Subclass Members and induce them to rely on its misrepresentations and omissions.

653. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

654. Had Defendants disclosed to Plaintiff Woods and Texas Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Woods and the Texas Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Woods and Texas Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

655. Defendants had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff Woods and the Texas Subclass, and Defendants because consumers are unable to fully protect their interests regarding their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully

withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

656. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

657. Consumers, including Plaintiff Woods and Texas Subclass Members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience, or capacity to secure the PII in Defendants' possession or to fully protect their interests regarding their data. Plaintiff Woods and Texas Subclass Members lack expertise in information security matters and do not have access to Defendants' systems to evaluate its security controls. Defendants took advantage of its special skill and access to PII to hide its inability to protect the security and confidentiality of Plaintiff Woods' and Texas Subclass Members' PII.

658. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach which resulted from Defendants' unconscionable business acts and practices, exposed Plaintiff Woods and Texas Subclass Members to a wholly unwarranted risk to the safety of their PII and the security of their identity or credit and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass Members cannot mitigate this unfairness because they cannot undo the Data Breach.

659. Defendants acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff Woods' and Texas Subclass Members' rights.

660. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiff Woods and Texas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach. Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiff Woods' and Texas Subclass Members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

661. Defendants' violations present a continuing risk to Plaintiff Woods and Texas Subclass Members as well as to the public.

662. Plaintiff Woods and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

COUNT XXVI
UTAH CONSUMER SALES PRACTICES ACT
Utah Code §§ 13-11-1, *et seq.*
(On behalf of Plaintiff Helvey and the Utah Subclass)

663. Plaintiff Helvey individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

664. Defendants are each a "person," as defined by Utah Code § 13-11-1(5).

665. Defendants is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

666. Defendants engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Helvey's and Utah Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Data Breach;

d. d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Helvey's and Utah Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Helvey's and Utah Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Helvey's and Utah Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Utah Protection of PII Act, Utah Code § 13-44-201.

667. Defendants intended to mislead Plaintiff Helvey and Utah Subclass Members and induce them to rely on its misrepresentations and omissions.

668. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

669. Had Defendants disclosed to Plaintiff Helvey and Utah Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures

and comply with the law. Defendants was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Helvey and the Utah Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Helvey and the Utah Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

670. Defendants had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff Helvey and the Utah Subclass, and Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff Helvey and the Utah Subclass that contradicted these representations.

671. Defendants intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

a. Indicating that the subject of a consumer transaction has approval, performance characteristics, accessories, uses, or benefits, if it has not;

b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;

c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not; and

d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (*e.g.* more data security) than the supplier intends.

672. Defendants engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Defendants' acts and practices unjustly imposed hardship on Plaintiff Helvey and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their PII. The deficiencies in Defendants' data security, and the material misrepresentations and omissions concerning those deficiencies, led to unfair surprise to Plaintiff Helvey and the Utah Subclass when the Data Breach occurred.

673. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Defendants to adequately secure PII in its possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff Helvey and the Utah Subclass and Defendants, which has control over the PII in its possession. Industry standards-including those reflected in the security requirements of the FTC and dictate that Defendants adequately secure the PII in its possession.

674. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiff Helvey and Utah Subclass Members have suffered and will continue to

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

675. Defendants' violations present a continuing risk to Plaintiff Helvey and Utah Subclass Members as well as to the public.

676. Plaintiff Helvey and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, et seq.; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XXVII
NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION
Wis. Stat. §§ 134.98(2), *et seq.*
(On behalf of Plaintiff Randall and the Utah Subclass)

677. Plaintiff Randall individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

678. Defendants is a business that maintains or licenses personal information (for the purpose of this count, "PII"), as defined by Wis. Stat. § 134.98(2).

679. Plaintiff Randall's and Wisconsin Subclass Members' PII (e.g., Social Security numbers) includes PII as covered under Wis. Stat. § 134.98(1)(b).

680. Defendants is required to accurately notify Plaintiff Randall and Wisconsin Subclass Members if it knows that PII in its possession has been acquired by a person whom it

has not authorized to acquire the PII within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

681. Because Defendants knew that PII in its possession had been acquired by a person whom it has not authorized to acquire the PII, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

682. By failing to disclose the Defendants data breach in a timely and accurate manner, Defendants violated Wis. Stat. § 134.98(2).

683. As a direct and proximate result of Defendants' violations of Wis. Stat. § 134.98(3)(a), Plaintiff Randall and Wisconsin Subclass Members suffered damages, as described above.

684. Plaintiff Randall and Wisconsin Subclass Members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT XXVIII
WISCONSIN DECEPTIVE TRADE PRACTICES ACT
Wis. Stat. § 100.18
(On behalf of Plaintiff Randall and the Utah Subclass)

685. Plaintiff Randall individually, and on behalf of the Utah Subclass, repeats and realleges all allegations if fully set forth herein.

686. Defendants are each a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

687. Plaintiff Randall and Wisconsin Subclass Members are members of "the public," as defined by Wis. Stat. § 100.18(1).

688. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Defendants to members of the public for sale, use, or distribution, Defendants made, published, circulated, placed before the public or caused (directly or

indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

689. Defendants also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

690. Defendants' deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Randall's and Wisconsin Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Randall's and Wisconsin Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Randall's and Wisconsin Subclass members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Randall's and Wisconsin Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

691. Defendants intended to mislead Plaintiff Randall and Wisconsin Subclass Members and induce them to rely on its misrepresentations and omissions.

692. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

693. Defendants had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff and the Wisconsin Subclass-and Defendants, because consumers are unable to fully protect their interests about their data and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

694. Defendants' failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

695. Defendants acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Randall's and Wisconsin Subclass Members' rights.

696. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiff Randall and Wisconsin Subclass Members have sufferefd and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

697. Defendants had an ongoing duty to all Defendants customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

698. Plaintiff Randall and Wisconsin Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

COUNT XXIX
VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT,
Va. Code. Ann. §§ 18.2-186.6, *et seq.*
(On behalf of Plaintiff Covington and the Virginia Subclass)

699. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

700. Defendants are required to accurately notify Plaintiff Covington and members of the Virginia Subclass following discovery or notification of a breach of its data security system if unencrypted or unredacted personal information ("PII") was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identity theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

701. Defendants are entities that owns or licenses computerized data that includes PII as defined by Va. Code Ann. § 18.2-186.6(B).

702. Plaintiff Covington's and members of the Virginia Subclass' PII includes PII as covered under Va. Code Ann. § 18.2-186.6(A).

703. Because Defendants discovered a breach of its security system in which unencrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identity theft or another fraud, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

704. By failing to disclose the Defendants data breach in a timely and accurate manner, Defendants violated Va. Code Ann. § 18.2-186.6(B).

705. As a direct and proximate result of Defendants' violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff Covington and members of the Virginia Subclass suffered damages, as described above.

706. Plaintiff Covington and members of the Virginia Subclass seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT XXX
VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, *et seq.*
(On behalf of Plaintiff Covington and the Virginia Subclass)

707. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

708. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

709. Defendants are each a "person" as defined by Va. Code Ann. § 59.1-198.

710. Defendants are each a "supplier," as defined by Va. Code Ann. § 59.1-198.

711. Defendants engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Defendants advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment (such as furnishing credit reports to prospective employers).

712. Defendants engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Covington's and members of the Virginia Subclass' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Covington's and members of the Virginia Subclass' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Covington's and members of the Virginia Subclass' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Covington's and members of the Virginia Subclass' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Covington's and members of the Virginia Subclass' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

713. Defendants intended to mislead Plaintiff Covington and members of the Virginia Subclass and induce them to rely on its misrepresentations and omissions.

714. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Covington and members of the Virginia Subclass, about the adequacy of Defendants' computer and data security and the quality of the Defendants brand.

715. Had Defendants disclosed to Plaintiff Covington and members of the Virginia Subclass that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

716. Defendants were trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff Covington and members of the Virginia Subclass. Defendants accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Covington and members of the Virginia Subclass acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

717. Defendants had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers including Plaintiff Covington and members of the Virginia Subclass – and Defendants, because consumers are unable to fully protect their interests regarding their data, placed trust and confidence in Defendants.

718. Defendants' duty to disclose also arose from, *inter alia,* Defendants':

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

719. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain characteristics, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model;

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised; and

d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

720. Defendants acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff Covington and members of the Virginia Subclass' rights. An award of punitive damages would serve to punish Defendants for its wrongdoing, and warn or deter others from engaging in similar conduct.

721. As a direct and proximate result of Defendants' deceptive acts or practices, Plaintiff Covington and members of the Virginia Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

722. Defendants' violations present a continuing risk to Plaintiff Covington and members of the Virginia Subclass as well as to the general public.

723. Plaintiff Covington and members of the Virginia Subclass seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

COUNT XXXI
MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*
(On behalf of Plaintiff Kohrell and Minnesota Subclass)

724. Plaintiff Kohrell individually, and on behalf of the Minnesota Subclass, repeats and realleges all allegations if fully set forth herein.

725. Defendants, Plaintiff Kohrell, and Minnesota Subclass Members are each a "person" as defined by Minn. Stat. § 325F.68(3).

726. Defendants' services and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

727. Defendants engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

728. Defendants engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Kohrell's and the Minnesota Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass

Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Kohrell's and the Minnesota Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

729. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

730. Plaintiff Kohrell and Minnesota Subclass Members conferred a benefit on Defendants—their student loan payments—in reliance on Defendants' omissions. Had Defendants disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure Nelnet adequately secured consumers' PII, Plaintiff Kohrell and

Minnesota Subclass Members would not have provided their sensitive personal information to Defendants.

731. Defendants' fraudulent, misleading, and deceptive practices affected the public interest, including those affected by the Data Breach.

732. As a direct and proximate result of Defendants' fraudulent, misleading, and deceptive practices, Plaintiff Kohrell and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

733. Plaintiff Kohrell and Minnesota Subclass Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT XXXII
MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Minn. Stat. §§ 325D.43, *et seq.*
(On behalf of Plaintiff Kohrell and Minnesota Subclass)

734. Plaintiff Kohrell individually, and on behalf of the Minnesota Subclass, repeats and realleges all allegations if fully set forth herein.

735. By engaging in deceptive trade practices in the course of their businesses and vocations, directly or indirectly affecting the people of Minnesota, Defendants violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that their goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

736. Defendants' deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Kohrell's and the Minnesota Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Kohrell's and the Minnesota Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Kohrell's and the Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

737. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

738. Defendants intended to mislead Plaintiff Kohrell and Minnesota Subclass Members and induce them to rely on their misrepresentations and omissions.

739. Had Defendants disclosed to Plaintiffs and Class members that Defendants' data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received,

maintained, and compiled Plaintiff Kohrell's and Minnesota Subclass Members' PII as part of the services they provided without advising Plaintiff Kohrell and Minnesota Subclass Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Kohrell's and Minnesota Subclass Members' PII. Accordingly, Plaintiff Kohrell and Minnesota Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

740. Defendants acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Kohrell's and Minnesota Subclass Members' rights.

741. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendants' services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

742. Plaintiffs and Class Members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

COUNT XXXIII
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of the Nationwide Class, or alternatively, the State Subclasses)

743. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

744. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

745. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and statutory duties to reasonably safeguard its customers' sensitive personal information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs alleges that Defendants' data security practices remain inadequate.

746. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

747. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants continues to owe a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

748. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

749. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at Nelnet occurs, Plaintiffs and Class Members will

not have an adequate remedy at law, because not all of the resulting injuries are readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

750. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs at Nelnet, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

751. Issuance of the requested injunction will serve the public interest by preventing another data breach at Nelnet, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

Plaintiffs, on behalf of all others similarly situated, request that the Court enter judgment against Nelnet including the following:

A. Determining that this matter may proceed as a class action and certifying the Classes asserted herein;

B. Appointing Plaintiffs as representative of the applicable Classes and appointing Plaintiffs' counsel as Class counsel;

C. An award to Plaintiffs and the Classes of compensatory, consequential, statutory, restitution, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendants to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of

those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; (iv) timely notify consumers of any future data breaches; and (v) delete or destroy any legacy consumer data that it is not necessary to keep for business purposes;

E. Entering a declaratory judgment stating that Defendants owe a legal duty to secure its student loan borrowers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure sensitive personal information;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

DATED: this 10th day of March, 2023

/s/ Joel M. Carney

Joel M. Carney, #21922
Jeana L. Goosmann, #22545
Joseph V. Messineo, #21981
GOOSMANN LAW FIRM, PLC
17838 Burke Street, Ste. 250
Omaha, NE 68118
Telephone: (402) 280-7648
carneyj@goosmannlaw.com
goosmannj@goosmannlaw.com
messineoj@goosmannlaw.com

and

Ian W. Sloss
Steven L. Bloch
Zachary Rynar
SILVER GOLUB & TEITELL LLP

One Landmark Square, Floor 15
Stamford, Connecticut 06901
Telephone: (203) 325-4491
Fax: (203) 325-3769
isloss@sgtlaw.com
sbloch@sgtlaw.com
zrynar@sgtlaw.com

Christian Levis
Johnathan Seredynski
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Fax: (914) 997-0035
clevis@lowey.com
jseredynski@lowey.com

Anthony M. Christina
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
Fax: (914) 997-0035
achristina@lowey.com

Interim Co-Lead Class Counsel